SIEMENS

3GPP TSG SA WG3 Security **S3-010076**
joint S2/S3 meeting, Göteborg, 27 Feb 2001

An analysis of 3G TS 23.228 v170 "IP Multimedia Subsystem - Stage 2" from a security point of view

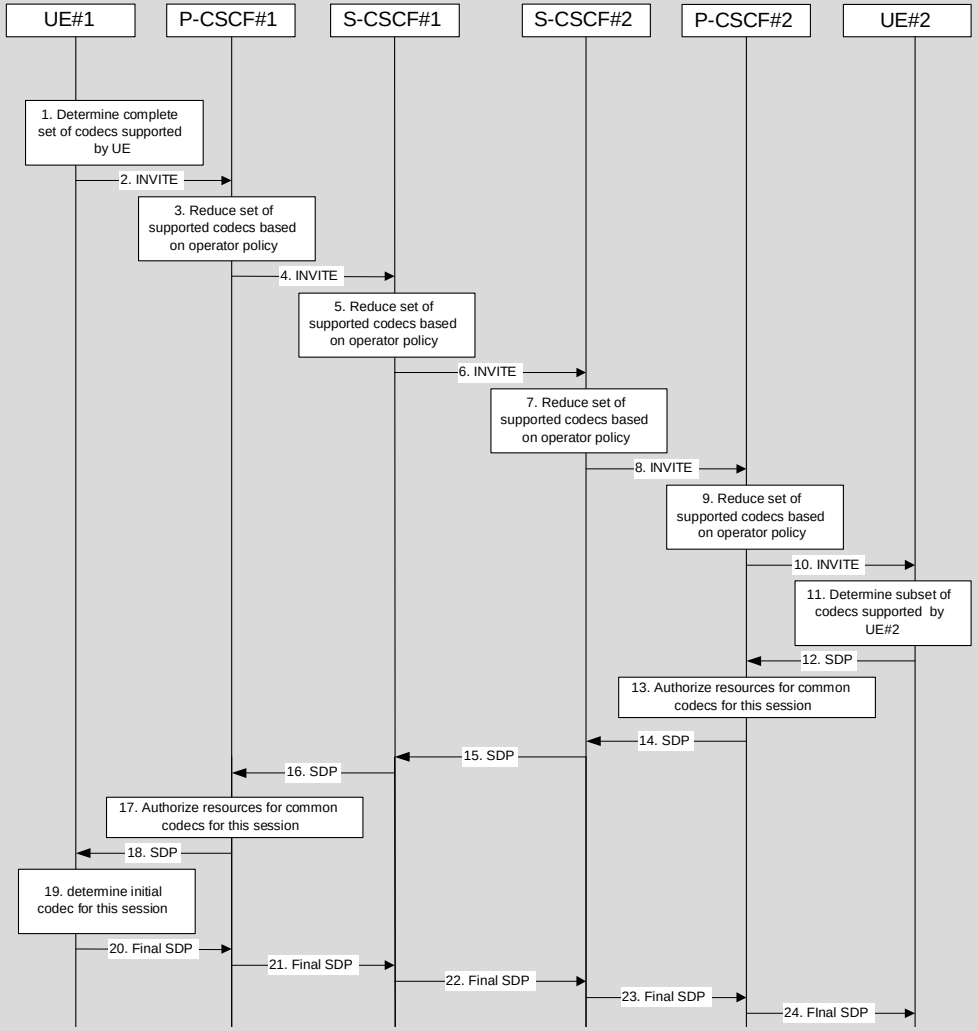
Source: **Siemens AG**

Document for: **Discussion**

Agenda item: **?**

SIEMENS

Information flow: Codec negotiation during initial session establishment (TS 23.228 v1.7.0, section 5.12.3.1)



Information flow: (in words) Codec negotiation during initial session establishment (TS 23.228 v1.7.0, section 5.12.3.1)

- **Extracted from TS 23.228 v1.7.0, section 5.12.3.1:**
  - This section gives information flows for the procedures for determining the set of mutually-supported codecs between the endpoints of a multi-media session, determining the initial codecs to be used for the multi-media session, and the procedures for changing between codecs when multiple ones are supported ...
  - 1. UE#1 determines the complete set of codecs that it is capable of supporting for this session. It builds a SDP containing bandwidth requirements and characteristics of each, and assigns local port numbers for each possible media flow. Multiple media flows may be offered, and for each media flow (m= line in SDP), there may be multiple codec choices offered.
  - 2. UE#1 sends the initial INVITE message to P-CSCF#1 containing this SDP
  - 3. **P-CSCF#1** examines the media parameters, and **REMOVES** any choices that the network operator decides, based on local policy, not to allow on the network.

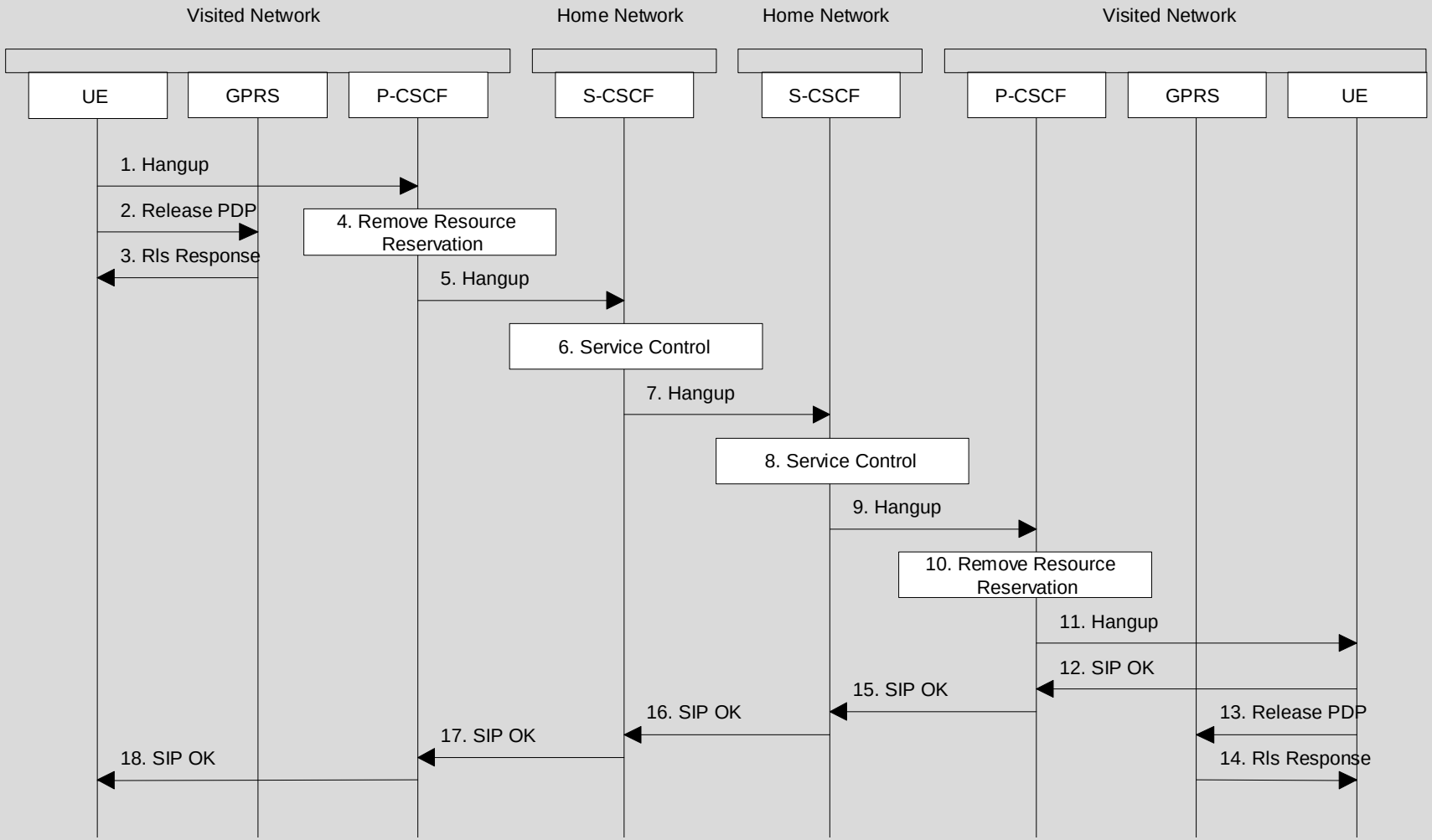
SIEMENS

Security analysis: Codec negotiation during initial session establishment (TS 23.228 v1.7.0, section 5.12.3.1)

- **Consequences:**
  - P-CSCF must be able to modify signalling messages sent by the UE in the procedures for codec negotiations

- **Conclusions:**
  - **These messages must not be integrity-protected between the UE and the S-CSCF**
  - **On the other hand, they should be integrity-protected between the UE and the P-CSCF again showing a need for integrity in the P-CSCF**

Information flow: Mobile terminal initiated session release (TS 23.228 v1.7.0, section 5.11.1)



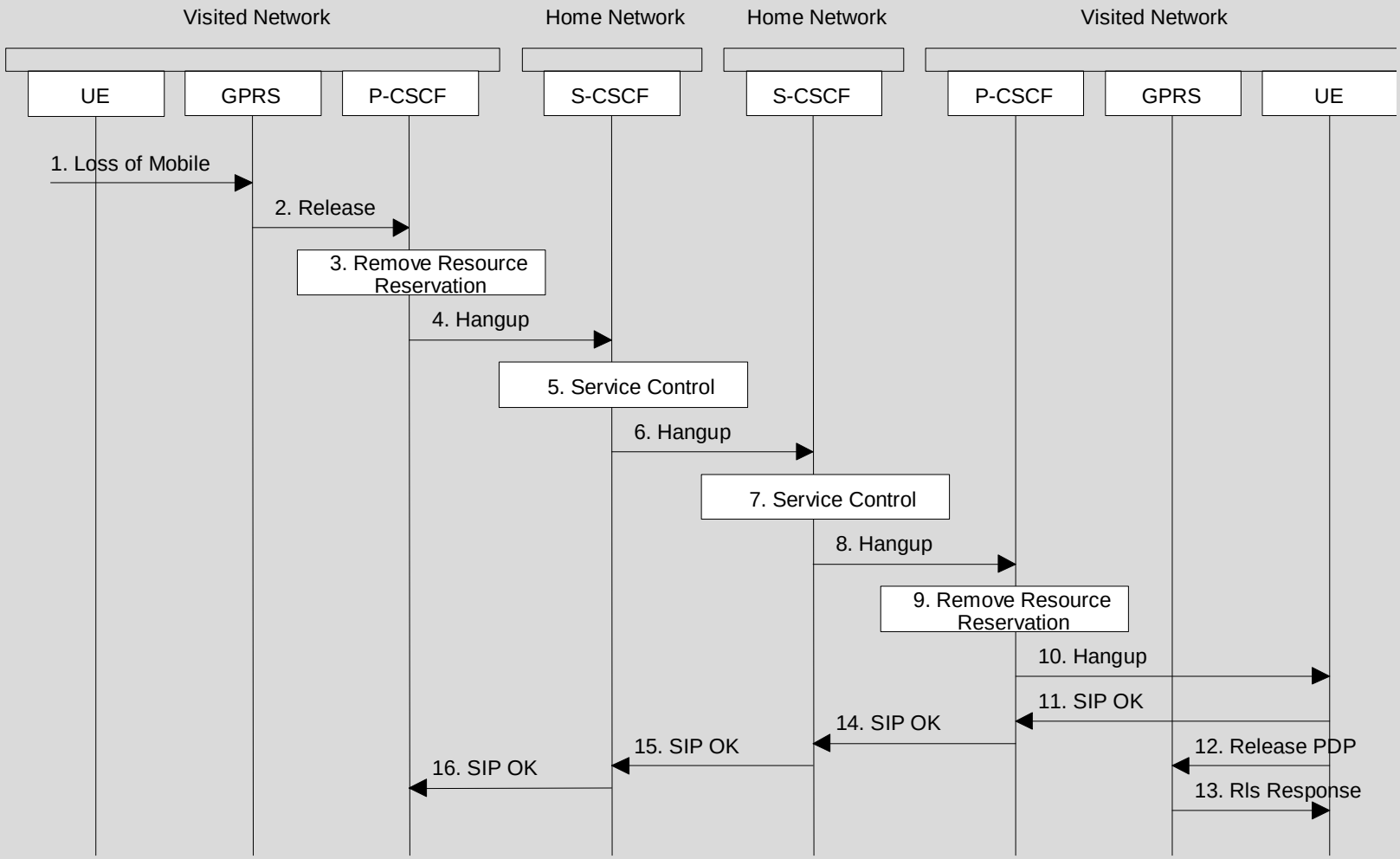
Information flow: Mobile terminal initiated session release (in words) (TS 23.228 v1.7.0, section 5.11.1)

- **Extracted from TS 23.228 v1.7.0, section 5.11.1:**
  - 1. One mobile party hangs up, which generates a message (Bye message in SIP) from the UE to the P-CSCF.
  - 2. Steps 2 and 3 may take place before or after Step 1 and in parallel with Step 4. The UE initiates the release of the bearer PDP context. The GPRS subsystem releases the PDP context. The IP network resources that had were reserved for the message receive path to the mobile for this call are now released. This is initiated from the GGSN. If RSVP was used to allocated resources, then the appropriate release messages for that protocol would invoked here.
  - 3. The GPRS subsystem responds to the UE.
  - 4. The **P-CSCF REMOVES THE AUTHORISATION FOR RESOURCES** that had previously been issued for this endpoint for this session. This step also will terminate the media flow if the UE did not properly perform that function in step 2 above.
  - 5. The **P-CSCF SENDS A HANG-UP** to the S-CSCF of the releasing party.

Security analysis: Mobile terminal initiated session release (TS 23.228 v1.7.0, section 5.11.1)

- **Consequences:**
  - Resources for the call are released before the S-CSCF even knows about it
  - If the P-CSCF is unable to verify the origin of the ”Bye” message sent by the UE then also a bogus ”Bye” message could cause the release of the call
  - In other words:
    - Anyone able to send IP packets to the P-CSCF could release anybody else’s call
    - This could be used to selectively target users or to cripple the system completely
  - **BUT:** procedure could be **modified** so that the P-CSCF releases resources after receiving confirmation from the S-CSCF. However, this would be at the **cost** of a **higher network signalling load** and a **higher delay** in releasing the resources.
- **Conclusions:**
  - **The P-CSCF should be able to check the integrity of release messages**

Information flow: Network initiated session release - P-CSCF initiated (TS 23.228 v1.7.0, section 5.11.3.1)



Information flow: Network initiated session release - P-CSCF initiated (in words) (TS 23.228 v1.7.0, section 5.11.3.1)

- **Extracted from TS 23.228 v1.7.0, section 5.11.3.1:**
  - 1. The bearer for the session is terminated, for example, by a mobile power down or loss of signal, etc. This is noted by the GPRS subsystem.
  - 2. The GPRS subsystem may send a release indication to the P-CSCF for the disconnected mobile. The P-CSCF might also note the release due to a SIP Session Timeout.

    Editor's Note: Which mechanism is used to report or detect release in this case is FFS.
  - The P-CSCF removes the authorisation for resources that had previously been issued for this endpoint for this session.
  - The P-CSCF generates a Hang-up (Bye message in SIP) to the S-CSCF of the releasing party. It is noted that this message should be able to carry a cause value to indicate the reason for the generation of the hang-up."

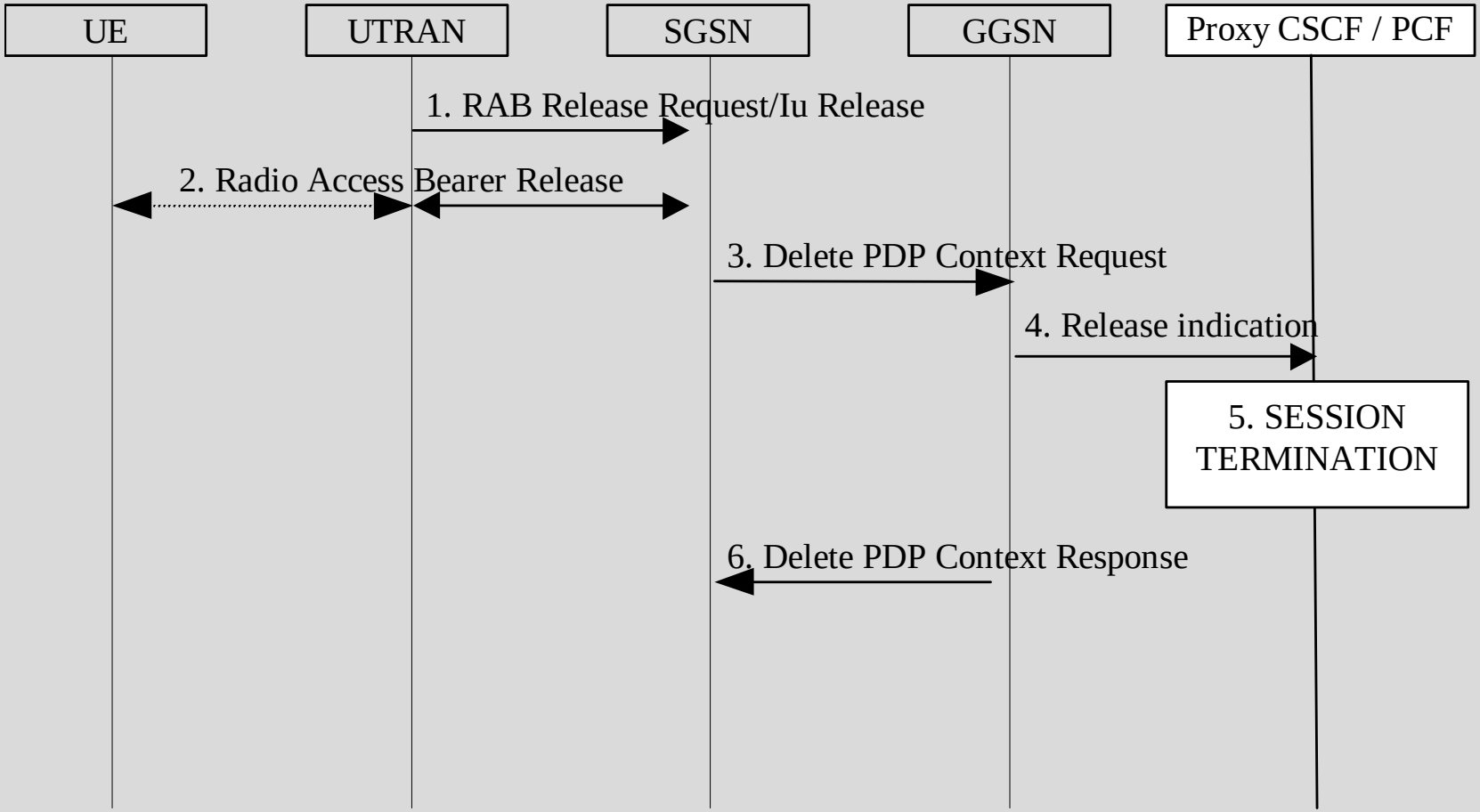
SIEMENS

Security analysis: Network initiated session release - P-CSCF initiated (TS 23.228 v1.7.0, section 5.11.3.1)

- **Consequences:**
  - Hang-up message is an example of a message sent by the P-CSCF to the S-CSCF which does not originate from the UE
  - S-CSCF must be able to check the integrity of this message so as to prevent fake session releases
  - Without protection the attacks would be the same as described for “Mobile terminal initiated session release”

- **Conclusions:**
  - Need for the **integrity between P-CSCF and S-CSCF independent of** any potential **integrity between UE and S-CSCF**
    - integrity between P-CSCF and S-CSCF **not user-specific**
    - may be provided according to”**Network Domain Security**”.
    - Shows that extending **integrity protection from UE to S-CSCF does not remove requirement for NDS**

Information flow: Network initiated session release (TS 23.228 v1.7.0, section 5.11.3)



Information flow: Network initiated session release (in words) (TS 23.228 v1.7.0, section 5.11.3)

- **TS 23.228 v1.7.0, section 5.11.3:**
  - ”In case of a break in the radio connection for a real-time PDP context which is related to an IM session, the corresponding session should be terminated in order to avoid billing for session inactivity time.
  - . . . . . .
  - 4. If a request state was created in the PCF [comment: Policy Control Function, located in P-CSCF] at PDP context activation, the GGSN sends the Release indication message to the PCF. The message indicates that the corresponding PDP context has been deactivated.
  - 5. The proxy CSCF performs session termination, which is FFS.”

Security analysis: Network initiated session release (TS 23.228 v1.7.0, section 5.11.3)

- **Consequences:**
  - This implies that anyone impersonating a GGSN towards a P-CSCF could terminate any session

- **Conclusions:**
  - **There is a need for integrity between GGSN and P-CSCF (not user-specific**)
  - May be provided according to"**Network Domain Security**"

Summary of Conclusions

- **Integrity-protection of all messages is not possible between the UE and the S-CSCF as the P-CSCF needs to modify payload of some of them**
- **P-CSCF should be able to check the integrity of messages sent by the UE**
- **Need for network domain security between GGSN and P-CSCF and between P-CSCF and S-CSCF**
- **General remark:**

  Perform integrity check of messages originating from the UE as early as possible so as to prevent bogus messages from creating additional load in the signalling network.

